SOCIAL SECURITY NUMBER AND PERSONALLY IDENTIFIABLE INFORMATION PROTECTION POLICY

Responsible CHA Department(s): Office of the General Counsel		**Policy No. 102.2**
Effective Date: May 17, 2022	Approved on 5/17/2022 by CHA Board of Commissioners Resolution No. 2022-CHA-17A	
This policy supersedes the Social Security Number Protection Policy (eff. 2018).		

I. Purpose.

The Chicago Housing Authority Social Security Number and Personally Identifiable Information Protection Policy ("Policy") establishes the requirements for compliance with the Illinois Identity Protection Act, 5 ILCS 179/1 *et seq*. (the "Act"), HUD Notice PIH-2015-06, 24 C.F.R. § 5.212, and the Illinois Personal Information Protection Act, 815 ILCS 530/1 ("PIPA"), to ensure the confidentiality and integrity of Social Security Numbers and Personal Information collected, maintained and used by the Chicago Housing Authority. The Policy establishes required handling and protection procedures for its Board members, employees, consultants, contractors, and volunteers and other authorized individuals with access to Social Security Numbers and Personal Information of Chicago Housing Authority employees, applicants, residents, and participants.

II. General Provisions.

A. Definitions.

1. "Authorized Individual" means any individual who is authorized to collect, use, or access Social Security Numbers ("SSNs") or Personally Identifying Information (or "PII," as defined in subsection II.A.12-13. below) by the Chicago Housing Authority, including, but not limited to, Employees, Officers, Volunteers, Contractors.

2. "Breach" means unauthorized acquisition of computerized data or hard copy documents that compromises the security, confidentiality, or integrity of SSNs and PII maintained by the Chicago Housing Authority or Contractor. "Breach" does not include good faith acquisition of an SSN or PII by an Authorized Individual for a legitimate purpose of the Chicago Housing Authority, provided that the SSN or PII is not used for a purpose unrelated to the Chicago Housing Authority's business or subject to further unauthorized disclosure.

3. "CHA" means the Chicago Housing Authority.

4. "CLO" shall mean the Chief Legal Officer of the CHA's Office of the General Counsel.

5. "Contractor" means a person who or entity that enters into a contract with the CHA, including their officers, employees, agents, sub-contractors, or consultants.

6. "Employee" means any individual in the employ of the CHA.

7. "Health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any medical information in an individual's health insurance application and claims history, including any appeals records.

8. “HUD” shall mean the U.S. Department of Housing and Urban Development Office of Public and Indian Housing.

9. “Income information” means information relating to an individual's income, including:

    a. All employment income information known to current or previous employers or other income sources that HUD or the processing entity determines is necessary for purposes of determining an assistance applicant's or participant's eligibility for, or level of assistance in, a covered program;

    b. All information about wages, as defined in the State's unemployment compensation law, including any Social Security Number; name of the employee; quarterly wages of the employee; and the name, full address, telephone number, and, when known, Employer Identification Number of an employer reporting wages under a State unemployment compensation law;

    c. With respect to unemployment compensation:

        (i) Whether an individual is receiving, has received, or has applied for unemployment compensation;

        (ii) The amount of unemployment compensation the individual is receiving or is entitled to receive; and

        (iii) The period with respect to which the individual actually received such compensation.

    d. Unearned IRS income and self-employment, wages and retirement income as described in the Internal Revenue Code, 26 U.S.C. 6103(l)(7); and

    e. Wage, social security (Title II), and supplemental security income (Title XVI) data obtained from the Social Security Administration.

10. "Medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional, including such information provided to a website or mobile application.

11. “Officer” means any appointed officer of the CHA, including members of CHA’s Board of Commissioners.

12. “Personally Identifiable Information” or “PII” as to applicants, residents, and participants means any of the following:

a. Information about an applicant, resident, or participant which can be used to distinguish or trace the applicant, resident, or participant's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.;

b. "Sensitive PII", which is personally identifiable information of an applicant, resident, or participant that when lost, compromised or disclosed without authorization could substantially harm the applicant, resident, or participant. Examples of Sensitive PII include social security or driver's license numbers, medical records, and financial account numbers such as credit or debit card numbers;

c. Income information in or related to an application, income verification, or verification for housing assistance or continued housing assistance; and,

d. Employer Identification Number ("EIN")

13. "Personally Identifiable Information" or "PII" as to individuals *other than* applicants, residents, and participants, as described in subparagraph 12 above, means any of the following:

a. Social Security Number ("SSN").

b. An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security:

c. Driver's license number or State identification card number;

d. Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;

e. Medical information;

f. Health insurance information; or

g. Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

h. User name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted

but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.

14. “PII,” whether for applicants, residents, participants or other individuals, does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

15. “Volunteer” means any person who donates their time to the CHA, whether or not they receive a stipend or in-kind benefit, including residents and participants, who may have access to SSNs and PIIs.

B. Applicability.

1. This Policy applies to CHA Board members, employees, consultants, contractors, and volunteers and other authorized individuals with access to Social Security Numbers and Personal Information of CHA employees, applicants, participants, and residents.

2. This Policy applies to any work product contracted for by the CHA with a Contractor, including work papers, reports, spreadsheets, data, data-bases, documentation, training materials, drawings, photographs, film and all negatives, software, tapes and the masters thereof, prototypes, and other material related thereto which contain an SSN or PII. Contractors shall comply with all aspects of this Policy and all applicable law, including the Illinois Personal Information Protection Act, 815 ILCS 530/1 et seq.

3. This Policy shall not apply to the collection, use or disclosure of an SSN or PII as required by state or federal law, rule or regulation, or the use of an SSN, PII, or other identifying information for internal verification or administrative purposes.

4. This Policy shall not apply to documents that are recorded with a county recorder or required to be open to the public under any state or federal law, rule or regulation, applicable case law, Supreme Court rule or the Constitution of the State of Illinois.

5. This Policy shall not apply to disclosure of criminal records utilized pursuant to 24 C.F.R. 5.903(e)(2) or any other applicable statute, rule, or regulation.

6. In the event any statute, rule, or regulation which HUD requires the CHA to follow as to the collection, use or disclosure of SSNs, PII, or any other personal information is stricter than the standards under this Policy, the stricter standards required by HUD shall control.

7. This Policy will be strictly enforced. Any deviations from the Policy must be justified in writing and approved by the CLO

III. Prohibited Activities.

a. General Prohibited Activities. No Employee, Officer, Contractor, or Authorized Individual shall do any of the following:

1. Publicly post or publicly display in any manner an individual's SSN or PII. "Publicly post" or "publicly display" means to intentionally communicate or otherwise

intentionally make available to the general public, including but not limited to physical or virtual means.

2. Print an individual's SSN on any card required for the individual to access products or services provided by the CHA.

3. Require an individual to transmit an SSN over the Internet or via e-mail, unless the connection is secure or the SSN is encrypted.

4. Print an individual's SSN on any materials that are mailed to the individual, through the U.S. Postal Service, any private mail service, electronic mail, or any similar method of delivery ("mail"), unless State or federal law requires the SSN to be on the document to be mailed. SSNs may be included in applications and forms sent by mail, including, but not limited to, any material mailed in connection with the administration of the Unemployment Insurance Act, any material mailed in connection with any tax administered by the Department of Revenue, and documents sent as part of an application or enrollment process or to establish, amend, or terminate an account, contract, or policy or to confirm the accuracy of the SSN.

5. Any SSN or PII that is permissibly mailed will not be printed, in whole or in part, on a postcard or other mailer that does not require an envelope or that can be visible on an envelope without the envelope having been opened. Materials with SSNs or PII will not be sent via interoffice mail.

b. Additional Prohibited Activities. In addition, no Employee, Officer, Contractor, or Authorized Individual shall do any of the following:

1. Collect, use or disclose an SSN from an individual, unless:

a. required to do so under State or federal law, rules, or regulations, or the collection, use, or disclosure of the SSN is otherwise necessary for the performance of the Employee's duties and responsibilities;

b. the need and purpose for the SSN is documented before or in connection with the collection of the SSN; and

c. the SSN collected is relevant to the documented need and purpose.

2. Use SSNs or PII for any purpose other than the purpose for which it was collected.

3. Require an individual to use his or her SSN to access an Internet website.

c. Exceptions. The prohibitions in subsections III.A. and III.B. above do not apply to the following circumstances:

1. The disclosure of SSNs or PII to agents, employees, contractors, or subcontractors of a governmental entity or disclosure by a governmental entity to another governmental entity or its agents, employees, contractors, or subcontractors if disclosure is necessary in order for the entity to perform its duties and responsibilities; and, if disclosing to a contractor or subcontractor, prior to such disclosure, the governmental entity must first receive from the contractor or subcontractor a copy of the contractor's or subcontractor's policy that sets forth how the requirements imposed under the Act on a governmental entity to

protect an individual's SSN will be achieved.

2. The disclosure of SSNs or PII pursuant to a court order, warrant, or subpoena, or in a court or administrative proceeding as allowed by applicable statute, rule, or regulation.

3. The collection, use, or disclosure of SSNs in order to ensure the safety of: State and local government employees; CHA employees; persons committed to correctional facilities, local jails, and other law enforcement facilities or retention centers; wards of the State; and all persons working in or visiting a CHA facility.

4. The collection, use, or disclosure of SSNs or PII for internal verification or administrative purposes.

5. The disclosure of SSNs to any entity for the collection of delinquent child support or of any State debt or to a governmental agency to assist with an investigation or the prevention of fraud.

6. The collection or use of SSNs or PII to investigate or prevent fraud, to conduct background checks, to collect a debt, to obtain a credit report from a consumer reporting agency under the federal Fair Credit Reporting Act, to undertake any permissible purpose that is enumerated under the federal Gramm Leach Bliley Act, or to locate a missing person, a lost relative, or a person who is due a benefit, such as a pension benefit or an unclaimed property benefit.

IV. Protections.

A. Limited Access. Only Employees, Officers, Contractors, and Authorized Individuals who are required to use or handle information or documents that contain SSNs or PII will have access. SSNs or PII shall only be shared or discussed with personnel who have a need to know the SSN or PII for purposes of their work. Employees, Officers, Contractors, and Authorized Individuals with access to SSNs or PII shall take all reasonable steps to keep unauthorized persons from overhearing or otherwise obtaining access to the SSNs or PII.

B. Training. All Employees, Officers, and Authorized Individuals identified as having access to SSNs or PII in the course of performing their duties shall be trained to protect confidentiality of SSNs and PII. Training shall include instructions on the proper handling of information that contains SSNs or PII from the time of collection through the destruction of the information. Contractors shall train any employees, officers, agents, or subcontractors who will have access to SSNs and PIIs to protect the confidentiality of SSNs and PII, and shall implement and maintain reasonable security measures to protect SSNs and PII from unauthorized access, acquisition, destruction, use, modification, or disclosure.

C. Documentation and Authorization of Need. No Employee, Officer, Contractor, or Authorized Individual shall collect, store, use or disclose an individual's SSN or PII unless authorized by the CEO or their designee or as is necessary for the performance of their duties.

D. Redacting. SSNs and PII requested from an individual shall be provided in a manner that makes the SSN and PII easily redacted if required to be released as part of a public records request.

E. Statement of Purpose(s). When collecting an SSN or upon request by the individual, a statement of purpose or purposes for which the CHA is collecting and using the SSN shall be provided.

F. Additional Protections. SSN information shall not be maintained on an unsecured portable electronic device and may not be transmitted via e-mail to third-parties unless encrypted in accordance with the requirements specified by the CLO. Employees, Officers, Contractors, and Authorized Individuals should endeavor to protect the confidentiality of electronic files and hard copies containing SSNs or PII.

G. Collecting and Maintaining Sensitive PII. Sensitive PII shall not be collected or maintained without proper authorization. Sensitive PII may only be collected as needed for its intended purpose. Sensitive PII shall only be shared or discussed with those personnel who have a need to know for purposes of their work. No Sensitive PII shall be left on a voicemail. Sensitive PII should not be discussed if there are unauthorized personnel, Contractors, or guests in adjacent cubicles, rooms, or hallways who may overhear the conversation. Meetings where Sensitive PII will be discussed shall be held in a secure space (*i.e*., limited access). Notes and minutes which contain Sensitive PII shall be treated as confidential. Physical and electronic files containing Sensitive PII shall be appropriately labeled. Physical files and electronic media containing Sensitive PII shall be secured and not left unattended. Digital copies of files containing Sensitive PII shall be secured (*e.g*. via encryption or two-factor authentication). Sensitive PII shall be stored only at workstations that can be secured. Records with Sensitive PII shall not be removed from facilities where it is authorized to be stored unless approval is first obtained from a supervisor. Sufficient justification, as well as evidence of information security, must be presented for approval to remove Sensitive PII.

H. Transmitting Sensitive PII. Employees, Officers, Contractors, and Authorized Individuals shall endeavor to protect the confidentiality of electronic files and hard copies when transmitting Sensitive PII via U.S. Postal Service, facsimile, or email in accordance with procedures established by the CLO. Sensitive PII shall not be transmitted via an unsecured information system (e.g. electronic mail, Internet, or electronic bulletin board) without first encrypting the information. Sensitive PII shall not be placed on or in unsecured locations. To the extent that Sensitive PII is contained in electronic files that are required to be placed on the Internet, such as via electronic filing of court documents, the Sensitive PII shall first be redacted.

V. Public Inspections and Copying of Documents.

Employees, Officers, Contractors, and Authorized Individuals shall comply with the provisions of any State law with respect to allowing the public inspection and copying of information or documents containing all or any portion of an individual's SSN and PII. In such cases, Employees, Officers, Contractors, and Authorized Individuals shall redact SSNs and PII from the information or documents before allowing the public inspection or copying of the information or documents.

VI. Compliance with Federal Law.

If a federal law takes effect requiring any federal agency to establish a national unique patient health identifier program, the CHA's compliance with federal law shall be deemed compliance with the Act and this Policy.

VII. Embedded Social Security Numbers.

Employees, Officers, Contractors, and Authorized Individuals shall not encode or embed an SSN in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, RFID technology or other technology, in place of removing the SSN.

VIII. Policy Violations and Breaches.

If an Employee, Officer, Contractor, or Authorized Individual discovers or reasonably believes that any provision of this Policy has been violated or that there has been a Breach, then the Employee, Officer, Contractor, or Authorized Individual shall immediately notify their supervisor, or CHA contact in the case of a Contractor. The supervisor or contact shall then immediately notify the head of their Department and the CHA's CLO. The CLO shall then take all steps deemed necessary to comply with applicable law.

IX. Disposal of Materials Containing Social Security Numbers or Personal Information.

An Employee, Officer, Contractor, or Authorized Individual shall dispose of any material containing an SSN, PII, or other personal data in accordance with the CHA's Records and Email Management and Retention Policy.

X. Authorization to Formulate Guidelines and Procedure.

The CLO is authorized to issue guidelines and procedures for the effective implementation of the requirements of this Policy as it relates to SSNs or PII collected by Employees, Officers, Contractors, or Authorized Individuals.

XI. Compliance.

Failure to abide by this Policy or guidelines will subject Employees, Officers, Contractors, and Authorized Individuals to discipline and/or sanctions up to and including dismissal or termination of contract in accordance with the CHA's disciplinary policies and debarment in accordance with the CHA's policies.

References: Illinois Identity Protection Act, 5 ILCS 179/1 *et seq.;* Illinois Personal Information Protection Act, 815 ILCS 530/1 *et seq*.; HUD Notice PIH-2015-06; 24 C.F.R. § 5.212
Policy History: Approved on 6/19/2018 by 2018CHA42 Revised on 5/17/2022